ChatGPT

Documentación de la API `generate_token` de Izipay

Descripción general

El endpoint **Crear token de sesión** (operación `generate_token`) permite generar un **token de sesión** que se utiliza como mecanismo de autenticación en las otras APIs de Izipay [1]. Este token es de un solo uso y su tiempo de vida es limitado (la documentación menciona una vigencia aproximada de 15 minutos en un recuadro de advertencia).

Este servicio es esencial para inicializar operaciones de ventas, tokenización, link de pago, anulaciones y depósitos. También se utiliza para la API de devoluciones cuando se especifica como fuente de solicitud `REFUND` [1].

URL del servicio

- **Entorno de pruebas (sandbox)**: `https://sandbox-api-pw.izipay.pe/security/v1/Token/Generate` [1].
- Método HTTP: **POST** [1].

Para producción, el dominio cambia a `https://api-pw.izipay.pe` y el resto de la ruta permanece igual.

Autenticación y encabezados

- **transactionId** (obligatorio): Identificador único para cada transacción generada por el comercio. Debe ser un valor de **5 a 40 caracteres** y debe coincidir con el valor utilizado al generar otros tokens [2].

Cuerpo de la solicitud (JSON)

Campo	Tipo	Requerido	Descripción	Restricciones / Ejemplo
`requestSource`	string	Sí	Origen de la petición. Puede tomar los valores `ECOMMERCE` o `REFUND`. `ECOMMERCE` se usa para las APIs de ventas, tokenización, link de pago, anulaciones y depósitos; `REFUND` se usa para la API de devoluciones [2].	6–10 caracteres. Ejemplo: `ECOMMERCE` [2]
`merchantCode`	string	Sí	Código del comercio o del sub-merchant (código hijo del merchantFacilitator) generado por Izipay durante la afiliación [3].	1–15 caracteres. Ejemplo: `4007701` [3]
`orderNumber`	string	Sí	Número de pedido de la operación [3].	5–15 caracteres. Ejemplo: `R2022111015` [3]
`publicKey`	string	Sí	Llave pública asociada a la generación del token; también llamada **Clave API Nuevo Botón de Pagos**. Puede obtenerse en la sección de **Recursos/ Credenciales** de la plataforma Izipay [3].	16–400 caracteres. Ejemplo: `VErEthUtraQUxas57wUMuquprADrAHAb` [3]

Campo	Tipo	Requerido	Descripción	Restricciones / Ejemplo
`amount`	string<decimal>	Sí	Monto de la operación. Para operaciones que no implican depósito se puede enviar `0.00`. Se utiliza un punto (.) como separador decimal, sin delimitador de miles [3].	4–13 caracteres. Ejemplo: `15.00` [3]

Ejemplo de solicitud con `curl`

```
curl --request POST   --url https://sandbox-api-pw.izipay.pe/security/v1/
Token/Generate   --header 'Accept: application/json'   --header 'Content-
Type: application/json'   --header 'transactionId: 16868479028040'   --data
'{
    "requestSource": "ECOMMERCE",
    "merchantCode": "4007701",
    "orderNumber": "R202211101518",
    "publicKey": "VErEthUtraQUxas57wUMuquprADrAHAb...",
    "amount": "15.00"
  }'
```

Estructura de la respuesta

En caso de éxito (HTTP 200), la respuesta tiene formato JSON y contiene:

- **code**: Código de respuesta de la autorización (normalmente `"00"` para indicar aprobación) [4].
- **message**: Mensaje asociado al código de autorización (por ejemplo, `"OK"`) [4].
- **response**: Objeto que incluye el **token** generado. Este token es una cadena alfanumérica larga (generalmente más de 255 caracteres) y es válido para un único uso [5].

El token debe incluirse en el encabezado `Authorization` al invocar otros endpoints de Izipay.

Códigos de respuesta

Código HTTP	Significado	Comentarios
200	Éxito	La solicitud se ha procesado correctamente y se devuelve un token válido [4].
4xx	Error del cliente	Por ejemplo, `400 Bad Request` cuando falta un parámetro requerido o `401 Unauthorized` cuando `transactionId` o la clave pública no son válidos.

Código HTTP	Significado	Comentarios
500	Error del servidor	Indica un problema interno al procesar la solicitud.

Buenas prácticas

1. **Generar un** `transactionId` **único** para cada solicitud. Esto facilita el seguimiento y auditoría de las llamadas.
2. **Proteger las credenciales**: La autenticación utiliza tokens **Bearer**; asegúrese de mantener en secreto la clave pública y el token generado. El portal recomienda no publicar estas claves en repositorios públicos [1].
3. **Definir el** `requestSource` **apropiado**: Use `ECOMMERCE` para la mayoría de las operaciones (ventas, tokenización, link de pago) y `REFUND` para la API de devoluciones [2].
4. **Manejo de errores**: Implemente lógica para interpretar los códigos de error HTTP y los mensajes de la respuesta, de modo que pueda informar de manera clara al usuario final o reintentar la operación.
5. **Rotación de tokens**: Dado que el token tiene vigencia limitada (aprox. 15 minutos), genere uno nuevo cuando sea necesario y no reutilice tokens caducados.

Referencias

La información anterior proviene de la documentación oficial de Izipay para el endpoint **Crear token de sesión** (`generate_token`) [1] [2]. Esta API forma parte de la sección **Seguridad** del portal Izipay Developers y se utiliza para autenticar llamadas a otros servicios.

---

[1] [2] [3] [4] [5] APIs | izipay developers
https://developers.izipay.pe/api/%23/operations/generate_token